Revista Brasileira de Direito Civil em Perspectiva

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 22.11.2019
Aprovado em: 04.12.2019

OS DIREITOS DA PERSONALIDADE FRENTE À SOCIEDADE DE VIGILÂNCIA: PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E CONSENTIMENTO NAS REDES SOCIAIS

Ramon Silva Costa[*]
Samuel Rodrigues de Oliveira[**]

Resumo:
As redes sociais captam nossas personalidades pelos rastros digitais que deixamos ao utilizá-las. A Lei brasileira 13.709/2018 (LGPD) regula o tratamento de dados pessoais, visando à proteção das pessoas. Assim, o trabalho questiona: de que forma o consentimento dos titulares dado às redes sociais pode se adequar à lei? O objetivo é compreender como as redes sociais afetam nossos direitos. A metodologia consiste em uma revisão bibliográfica e análise legislativa. Conclui-se que o consentimento é um mecanismo capaz de conferir a autodeterminação informativa aos usuários, que precisam estar cientes sobre como suas informações pessoais são tratadas.

Palavras-chave: Sociedade de Vigilância; Dados Pessoais; Redes Sociais; Privacidade; Consentimento.

PERSONALITY RIGHTS IN THE SOCIETY OF SURVEILLANCE: PRIVACY, PERSONAL DATA PROTECTION AND CONSENT ON SOCIAL NETWORK

Abstract:
Social Networks capture our personalities through the digital tracks we leave when using them. The Brazilian Law 13.709 / 2018 (LGPD) regulates the processing of personal data, aiming at the protection of people. Thus, the paper asks: how can the consent of the holders given to social networks fit the law? The goal is to understand how social networks affect our rights. The methodology consists of a literature review and legislative analysis. It is concluded that consent is a mechanism capable of conferring informative self-determination to users who need to be aware of how their personal information is treated.

Keywords: Surveillance Society; Personal data; Social Networks; Privacy; Consent.

INTRODUÇÃO

[*] Graduado em Direito pela Universidade Federal Fluminense (UFF) e mestrando bolsista CAPES em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF).
CV: http://lattes.cnpq.br/6927532056597666
Endereço eletrônico: ramoncostta@outlook.com. Endereço postal: Rua José Lourenço Kelmer, s/n, Faculdade de Direito- UFJF, São Pedro. CEP: 36036-900- Juiz de Fora-MG
[**] Graduado em Direito e mestrando em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF).
CV: http://lattes.cnpq.br/3924533920462594
Endereço eletrônico: samuelrdeoliveira@gmail.com. Endereço postal: Rua José Lourenço Kelmer, s/n – Faculdade de Direito, São Pedro. CEP: 36036-900 - Juiz de Fora- MG.

O documentário *Terms and Conditions my apply*[1] ("Sujeito a termos e condições"), do diretor americano Cullen Hoback, lançado em 2013, discute a expansão progressiva do mercado de dados alimentado pelos Estados e grandes corporações como *Facebook*, *Google* e *Amazon*[2] e nos alerta sobre as dimensões cada vez mais problemáticas para a tratativa jurídica desse mercado. Nossos dados já são vistos como "o novo petróleo", sendo imprescindíveis para as articulações mercadológicas na contemporaneidade. Como destaca Nick Srnicek (2018), o capitalismo do século XXI é estruturado pela *data-driven economy* (economia movida a dados), ou seja, os dados pessoais ocupam a centralidade em grande parte das atividades econômicas no contexto do capitalismo globalizado.

O documentário já nos indagava com questionamentos que ainda persistem e que estarão presentes neste artigo. Como proteger nossos dados pessoais? De que forma o consentimento fornecido aos controladores de dados pelos usuários de redes sociais pode ser mais eficaz e de acordo com a legalidade? Como a privacidade dos indivíduos se estrutura juridicamente em uma sociedade digital? De que forma temos nossos direitos de personalidade são violados pelas ações do mercado de dados?

O presente trabalho não pretende responder objetivamente todas essas questões, mas dá enfoque à função do consentimento na proteção de dados pessoais de usuários de redes sociais. Assim, questiona-se: como o consentimento proposto nos termos de uso das redes sociais pode adequar-se à Lei Geral de Proteção de Dados Pessoais (LGPD)? Dessa forma, o artigo se propõe a compreender como a digitalização de nossas relações sociais implica violações aos nossos direitos personalíssimos previstos no texto constitucional e tratados no Código Civil de 2002, assim como busca analisar de que maneira o consentimento presente nas redes pode conferir a autodeterminação informativa de seus usuários. Para tanto, será necessária uma contextualização acerca da evolução do conceito de privacidade nos tempos atuais e sua diferenciação em relação à proteção de dados pessoais, trazida pela LGPD (Lei 13.709/2018), que entrará em vigor em agosto de 2020.

A metodologia empregada consiste em uma pesquisa teórica exploratória. De acordo com Gil (2007), a pesquisa exploratória permite uma aproximação investigativa em torno do problema, o tornando mais explícito e facilitando o levantamento de hipóteses e dados para o pesquisador. Esse tipo de pesquisa depreende, em grande parte, métodos de análise

[1] Ver trailer em: < https://www.youtube.com/watch?v=ayOpCrPlLrU>.
[2] Empresa transnacional norte-americana de comércio eletrônico.

documental e revisão bibliográfica, que serão utilizados neste trabalho. A revisão bibliográfica conta com livros e artigos variados na temática sobre proteção de dados e sociedade digital, com destaque para uma avaliação dos estudos do jurista italiano Stefano Rodotá (2008), que norteará o texto como marco teórico na tratativa da privacidade na sociedade de vigilância. A análise documental visa a uma verificação e compreensão dos pressupostos legais dispostos na Lei Geral de Proteção de Dados Pessoais (LGPD) e no Ordenamento Jurídico Brasileiro, com ênfase em uma leitura contemporânea dos direitos de personalidade presentes na discussão acerca do uso de redes sociais.

Assim, o texto estrutura-se em quatro partes. A primeira destaca os desafios jurídicos em uma sociedade de vigilância e os processos de digitalização das relações humanas. Posteriormente, é dado enfoque a uma diferenciação entre direito à privacidade e proteção de dados pessoais no Brasil. A terceira parte versa sobre a tratativa da proteção de dados pessoais como parte dos direitos da personalidade e as dimensões desses direitos nas redes sociais. Em seguida, damos centralidade ao consentimento previsto nas redes sociais e às previsões da Lei Geral de Proteção de Dados Pessoais, identificando possíveis violações à personalidade dos usuários. Por fim, as considerações finais expõem conclusivamente o conteúdo disposto no artigo.

1. A SOCIEDADE DE VIGILÂNCIA

A digitalização de nossas experiências e relações sociais tem sido um processo constante, amparado pelo aprimoramento tecnológico dos dias atuais, com o surgimento de tecnologias cada vez mais ágeis, eficientes e com grande potencial de armazenamento e difusão de informações. O advento da internet foi observado pelo autor Piérre Levy (2001), a partir do ciberespaço, que é o novo meio de comunicação que surge da interconexão mundial dos computadores. O ciberespaço não compreende apenas a infraestrutura material da comunicação digital, mas também do universo de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Pode-se falar ainda em "cibercultura", que se configura como o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço (LÉVY, 2001, p.17).

Nesse sentido, as redes sociais como *Facebook, Instagram*[3], *Tinder*[4] e *Grindr*[5], estão localizadas em uma dimensão específica desse ciberespaço. Essas redes possibilitam novas formas de comunicação e interação entre as pessoas, por serem plataformas que diminuem a distância entre os indivíduos por meio de um processo de digitalização das relações humanas. Desejos, personalidades, comportamentos e condutas são redimensionados para as redes sociais, o que não significa o fim de nossas interações *off-line*, mas indica uma importância central do espaço digital em nossas formas de socialização.

No entanto, para além de um espaço que promove sociabilidades, as redes sociais são utilizadas pelas corporações como captadoras de dados pessoais de seus usuários. Há uma coleta de dados maciça, muitas vezes realizada sem o consentimento e conhecimento dos titulares desses dados. Segundo Ana Frazão (2019a, p. 26), se as pessoas não sabem sequer quais de seus dados são captados nas redes, há uma dificuldade ainda maior de compreenderem como esses dados, convertidos em informações sobre sua intimidade e personalidade, são utilizados pelas empresas e como esses usos impactam suas vidas.

De acordo com Stefáno Rodotà (2008, p. 13), em uma sociedade de vigilância questiona-se o fim da privacidade dos indivíduos, em virtude das exigências dos mercados contemporâneos e da montagem dos robustos bancos de dados pessoais. O autor observa que, após o atentado de 11 de setembro, as dimensões jurídicas acerca da privacidade foram afrouxadas mundo a fora, com a redução de garantias fundamentais por meio de diplomas legais como o *Patriot Act* nos Estados Unidos e até mesmo pelas decisões na Europa de liberação de dados de passageiros de linhas aéreas para os Estados Unidos. O mercado se aproveita desse processo de diminuição de garantias, sendo as novas oportunidades tecnológicas mecanismos eficientes para a classificação, seleção, triagem e controle de indivíduos por meio da coleta de seus dados pessoais (RODOTÀ, 2008, p. 14).

A sociedade da vigilância é pensada por Michael Foucault (1996) como a sociedade moderna, ou, em suas palavras, como a sociedade disciplinar. O autor enfatiza a constituição de uma hierarquia de poderes, na qual são criados mecanismos de vigilância como forma de

[3] Rede social lançada em 2010 que permite o compartilhamento de fotos e vídeos entre seus usuários e sua reprodução em uma variedade de serviços de redes sociais. Ver mais em: <https://www.instagram.com/about/us/>.

[4] Rede de relacionamento geolocalizada que utiliza dados do perfil do facebook de seus usuários. Ver mais em: < https://tinder.com/?lang=pt-BR>.

[5] Aplicativo geolocalizado para relacionamento entre homens, com enfoque no público gay. Ver mais em: <https://www.grindr.com/br/about/>.

controle dos vigiados, que produzem saberes sobre estes e controlam seus comportamentos e posicionamentos sociais. Sendo assim, a sociedade se caracteriza por um conjunto de ferramentas institucionais e sociais que legitimam disciplinas de vigilância sobre os indivíduos.

Essa vigilância social centra-se em um "olhar que vê sem ser visto", algo que nos é perceptível nas novas tecnologias de comunicação e suas redes sociais, nas quais os controladores de dados nos observam, recolhem e utilizam nossos dados pessoais, sem que tenhamos quaisquer tipos de ingerência nesse processo. A vigilância permite a produção de conhecimento sobre aqueles que são vigiados, sendo este um aspecto fundamental para o exercício do poder. Nesse contexto, poder e saber são coadunados para o controle expressivo de nossas vidas. Vigiar produz saber, e esse conhecimento sobre o objeto observado reforça as possibilidades de exercer poder sobre ele (FOUCAULT, 1996).

A autora Soshana Zuboff (2019, p. 8) indica que essa sociedade de vigilância implica o atual capitalismo de vigilância, que utiliza toda experiência humana, incluindo vozes, personalidades e emoções que estão contidas em nossos dados pessoais, controlados e capitalizados como dados comportamentais para os mais diversos mercados embasados nas informações que nos são retiradas de forma gratuita, por meio de nossos rastros digitais, deixados em nossas redes através de nossas pesquisas na internet, ou até mesmo pelos nossos registros de compra *on-line*.

Assim, a economia movida a dados e o capitalismo de vigilância estão imbricados de forma substancial, pois a extensão do mercado baseado em dados pessoais exige a expansão da vigilância. Nesse sentido, como aponta Bruno Bioni (2018, p. 48), os dados pessoais configuram-se como um "ativo econômico" na contemporaneidade, sendo o avanço tecnológico o propulsor da virtualização das informações como "fator crítico da atividade empresarial". Dessa forma, o capitalismo de vigilância se caracteriza pela utilização dos dados pessoais por governos, empresas e grandes corporações, que estruturam um conhecimento amplo sobre as informações pessoais dos cidadãos, culminando na ampliação dos aspectos de controle da sociedade de vigilância (PASQUALE, 2015, p. 43-44).

Os questionamentos acerca de uma regulamentação, ou de uma resposta jurídica aos efeitos da sociedade de vigilância sobre nossas relações pessoais, sociais e de consumo, perpassam os entendimentos sobre como a indústria de dados se constitui a partir de um ativo que não lhe pertence: nossos dados pessoais. Dados esses que frequentemente são captados de

forma ilícita, em um processo envolto por justificativas como uma suposta gratuidade dos serviços e vantagens prestados pelas empresas por meio de seus produtos, como as redes sociais. Nesses processos, os usuários muitas vezes não percebem que a "troca" de seus dados pela possibilidade de uso das redes os configura como os reais produtos dessas redes e não como parte com condições de equidade em uma relação de consumo (FRAZÃO, 2019a, p. 30).

Isso ocorre porque os dados pessoais são os registros de nossas atividades sociais, de nossa personalidade e de nossa intimidade, ou seja, os dados pessoais são registros que nos identificam e que refletem o que somos. Assim, nos oferecemos enquanto moeda de troca nesse mercado digital e nos disponibilizamos a uma série de violações a direitos fundamentais. Nesse sentido, evidencia Frazão:

> (...) o mercado de dados em geral cresce a partir da difusão de visões como a de que o modelo de negócios é justo, já que os usuários receberiam contrapartidas adequadas pelos seus dados, ou mesmo necessário, dado que haveria um verdadeiro *trade-off* entre inovação e privacidade, de maneira que a violação desta última seria o preço a pagar ou o mal necessário para o progresso tecnológico e os novos serviços que daí decorrem. Até a forma como a questão é apresentada já reflete a perspectiva utilitarista que permeia a análise, pois se parte da premissa de que, em nome da inovação, é justificável o sacrifício de direitos fundamentais elementares (FRAZÃO, 2019a, p. 31).

Portanto, a sociedade de vigilância se configura como um processo de exercício de poder dos vigilantes sobre os vigiados, sendo a fonte do poder as informações pessoais contidas em nossos dados disponibilizados nas mais diversas redes. É nesse contexto que a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) se faz presente, tendo o "importante papel de reforçar a autonomia dos titulares dos dados e o necessário e devido controle que estes precisam exercer sobre os seus dados", no intuito de limitar os excessos e ilicitudes que permeiam o mercado movido pelos dados pessoais (FRAZÃO, 2019a, p. 31).

2. O DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS

Segundo Danilo Doneda (2006, p. 126-127), a privacidade é historicamente compreendida a partir da dicotomia público-privado. O direito à privacidade sempre partiu de ideias sobre quais atividades deveriam ser exercidas na esfera pública e quais deveriam estar restritas ao espaço privado dos indivíduos, sendo limitado por uma compreensão de que a habitação dos indivíduos seria o local de refúgio do escrutínio público. Nesse sentido, Hannah

Arendt (2010, p. 77-85) compreende o direito à privacidade como pressuposto democrático, visto que a partir da fuga da "pressão social", os indivíduos podem vivenciar e experimentar suas subjetividades no espaço privado.

Sendo assim, há uma seleção entre as informações que podem ser partilhadas publicamente e aquelas que devem ser mantidas em sigilo. Desse modo, ainda que informações da vida íntima sejam compartilhadas com maiores ou menores números de pessoas, se restringem ao controle dos indivíduos e ao seu interesse de mantê-las distantes do público em geral. É nesse contexto que a privacidade pode ser compreendida como o direito de ser deixado só, ou seja, como uma garantia de não violação ou invasão de seus aspectos privativos, assim como o próprio artigo 5º, X da Constituição Federal e o artigo 21 do Código Civil preceituam, ao determinarem a vida privada como inviolável (BIONI, 2018, p. 95-96).

Nesse sentido, a privacidade pode ser encarada como um direito guiado pela liberdade negativa de seu titular, que decide sobre quais aspectos de sua vida estão contidos em sua esfera privada e que, portanto, são tutelados por esse direito (RODOTÀ, 2012, p. 320). No entanto, esse entendimento clássico sobre o direito à privacidade, também se mostra limitado para o cenário atual, pois a própria definição acerca da privacidade é incerta, levando a privacidade a um status de termo "guarda-chuva", de conceituação abstrata (SOLOVE, 2014, p. 44). Assim, Stefano Rodotà destaca a necessidade de ampliação do conceito de direito á privacidade em uma sociedade altamente digitalizada:

> Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem (RODOTÀ, 2008, p. 25).

Esse processo evolutivo do conceito de direito à privacidade vai desde a ideia de ser deixado em paz, até uma compressão de direito de controle sobre as informações pessoais e de construção da esfera privada. Dessa forma, a evolução do direito à privacidade envolveria a proteção de dados pessoais (RODOTÀ, 2008, p. 17). Logo, há uma transformação do

conceito, que passa a abarcar não só o poder de exclusão, de impedimento de interferências alheias, mas também a centralidade do controle do indivíduo sobre suas informações pessoais, ou seja, sua autodeterminação informativa.

Nesse cenário, a privacidade caminhou da sequência "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle" (RODOTÀ, 2008, p. 93). A ideia tradicional de privacidade deve relacionar-se com as novas dimensões contemporâneas que perpassam a esfera privada e as informações pessoais. Isso não significa, contudo, que a proteção de dados pessoais é uma simples extensão do processo evolutivo do conceito de privacidade. Ao contrário, indica que ela se estabelece como um direito autônomo, que necessita de clareza e especificidade normativa, pois, mesmo que a proteção de dados esteja relacionada, em alguns aspectos, à tutela da privacidade dos indivíduos, ela não está restrita a dicotomia do público e do privado. Nesse ponto, diferencia-se essencialmente do direito à privacidade, sendo um equívoco dogmático indicar a proteção de dados pessoais como uma mera evolução do direito à privacidade (BIONI, 2018, p. 98-99).

Em uma sociedade digital, o tratamento de dados tem se tornado cada vez mais expansivo e impacta cada vez mais pessoas e realidades sociais. Nesse contexto, portanto, a proteção de dados pessoais ergue-se como a tutela da "própria dimensão relacional da pessoa humana", pois existe um leque vasto de liberdades individuais relacionadas com a proteção de dados pessoais, que extrapolam os limites de tutela do direito à privacidade, pois este é atrelado a uma divisão das esferas pública e privada de seus titulares (BIONI, 2018, p. 99).

3. A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO DA PERSONALIDADE

A Constituição Federal de 1988 é um marco normativo da tutela dos direitos da personalidade por reconhecer o princípio da dignidade humana em seu artigo 1º, III. A Constituição também trouxe outras garantias como a liberdade de expressão (art. 5º, IX) e o direito à informação (art. 5º, XV). Segundo Gustavo Tepedino (2004, p. 47), os direitos da personalidade não precisam estar concentrados como um único direito subjetivo, ou representados a partir de múltiplas classificações, sendo a técnica mais apropriada, a de proteger amplamente a pessoa em todos os seus aspectos. Contudo, a dignidade humana seria uma cláusula geral de proteção das pessoas, pois está relacionada com os direitos

fundamentais e ambos atuam conjuntamente no centro do discurso jurídico constitucional, configurando-se como dispositivos indissociáveis e essenciais para qualquer ordem jurídica verdadeiramente democrática (PASQUALINI, 1999, p. 80-81).

Nesse sentido, o Direito Civil teve seu campo ampliado pelas disposições constitucionais, ocorrendo a centralidade da dignidade humana e da tutela dos direitos da personalidade dos indivíduos. Assim, a pessoa tornou-se o centro da tutela jurídica, especificamente pelos direitos da personalidade, o que imputa uma releitura do Direito Civil, em moldes contemporâneos e através de leituras civis-constitucionais. A partir dessa releitura do Direito Civil, o sujeito, até então lido como sujeito neutro, passa a ser compreendido enquanto pessoa humana, no qual está o foco de tutela de todo o ordenamento jurídico. No entanto, faz-se necessário uma coexistência dos sentidos de sujeito e pessoa, tanto para uma observação das diferenças, como para os casos em que um sentido de sujeito reforce parâmetros de igualdade e liberdade entre as pessoas (TEPEDINO, 2016, p.18-23).

Assim, os direitos da personalidade são aqueles direitos inerentes a elementos corpóreos e incorpóreos que caracterizam e diferenciam uma pessoa. Dentre os exemplos mais comuns encontrados no Código Civil temos o direito ao nome, à honra, à integridade física e psíquica. Desse modo, levando-se em conta a diferenciação entre as pessoas, o Direito nos protege de violações contra a individualidade (TEPEDINO, 2004, p. 29).

Na sociedade digital, as redes sociais constituem um cenário de novos desafios para a tutela da personalidade humana. A partir das atividades de controle e armazenamento de dados pessoais efetivadas pela economia de dados, as personalidades são mapeadas no espaço digital por "signos identificadores" das pessoas. É uma nova identidade que os controladores de dados precisam classificar, de acordo com a personalidade do titular das informações. Assim, entende-se a justificativa dogmática para a "inserção dos dados pessoais na categoria de direitos da personalidade" (BIONI, 2018, p.65).

Nesse contexto, Frazão (2019, p. 25) elucida que essa massa de dados pessoais, entregues ao controle das plataformas digitais, receberam aperfeiçoamentos de controle, armazenamento e utilização com o *Big Data*[6] e *Big Analytics*[7], sendo pouco provável uma compreensão acerca da dimensão do poder dos dados na sociedade contemporânea, embora

[6] Termo que se refere aos grandes conjuntos de dados que dependem de um controle extenso devido ao seu volume.
[7] Nome dado à análise de grandes volumes de dados, que são traduzidos em informações, geralmente por meio de algoritmos.

possamos vislumbrar o quão grande é. A autora enfatiza que no cenário de uma sociedade de vigilância, o *Big Data* vigia todos os nossos passos, sendo capaz de capturar todas as nossas pegadas digitais deixadas nos aparelhos ao utilizarmos a internet. Essa alta capacidade de vigilância confere às plataformas digitais o poder sobre nossas escolhas, nos influencia e nos limita em nossas atividades e experiências. Esse processo é feito totalmente às escuras, pois os algoritmos atuam sem transparência e *accountability*[8], com a justificativa de serem segredos de Estado para os governos e de negócios para as empresas (FRAZÃO, 2019a, p. 38).

As redes como *Google* e *Facebook*, entretanto, expressam que não recolhem dados relacionados ao nome de seus usuários, ou seja, trata dados anonimizados, que não necessariamente identificam os indivíduos em particular. De fato, a forma como a Internet funciona não implica uma necessidade de identificação direta dos usuários para lhes direcionar conteúdos ou classificar seu perfil em um processo de decisão automatizada. Esse processo pode ser feito pela identificação do protocolo de endereço (IP) dos computadores e aparelhos, que podem ter múltiplos usuários. A partir desse "identificador eletrônico", os dispositivos são reconhecidos e torna-se possível uma leitura do perfil comportamental da navegação on-line realizada (BIONI, 2018, p. 77-78).

Logo, a identificação do perfil comportamental da navegação registrada nos aparelhos pode ser feita a partir de um conjunto de dados de diversos indivíduos, como de uma família que usa o mesmo computador, o que impossibilita uma identificação pessoal específica. No entanto, isso não afeta o cerne da LGPD, que está na defesa do cidadão contra a excessiva exposição a violações nas redes, não sendo razoável uma divisão rígida entre dados pessoais e dados anonimizados, visto que a determinação de perfis comportamentais feita pelos controladores de dados geram efeitos violadores na vida das pessoas, sendo elas identificáveis ou não (POULLET, 2008, p. 23).

Ainda, o tratamento de dados anonimizados não impede que ocorram interferências no livre desenvolvimento da personalidade dos indivíduos, pois os algoritmos utilizados no controle e classificação de dados podem distinguir pessoas de formas discriminatórias (BAROCAS; SELBST, 2016, p. 2-6). Nesse sentido, a Lei Geral de Proteção de Dados Pessoais abrange sua tutela para todos os tipos de controle de dados pessoais, seja

[8] Termo que no presente contexto pode ser definido como a responsabilidade dos controladores de dados em prestar contas sobre como efetuam o tratamento de dados pessoais.

anonimizados ou não, que possam subordinar os cidadãos a decisões automatizadas, que possibilitem violações à personalidade de uma pessoa ou de uma coletividade. Assim, a Lei 13.709/2018 preconiza em seu art. 12, § 2º que os dados anonimizados podem ser considerados dados pessoais, quando utilizados na construção de perfis comportamentais.

Os dados pessoais configuram-se como uma extensão da personalidade, constituem elementos substanciais de nossa singularidade, por isso podem ser compreendidos como reflexos pessoais capazes de nos identificar em nossas particularidades e enquanto seres sociais. Disso decorre a importância de elevar a proteção de dados pessoais a um *status* de direito da personalidade, que inclusive está em vias de ser incluído na gama de nossos direitos fundamentais pela PEC 17/2019[9]. A importância de uma normatização mais eficiente e que abarque da forma mais extensa possível a tutela da personalidade deve-se ao fato de que a exploração dos dados pessoais ultrapassa um simples sentido de violação à privacidade, principalmente se levarmos em conta a conceituação clássica de privacidade assentada no direito de ser deixado só. As violações que podem ocorrer em um contexto de controle irregular e ilegal de dados pessoais alcançam muitas outras esferas do cidadão, colocando em risco até mesmo sua autonomia e individualidade (FRAZÃO, 2019b, p. 100).

Portanto, a proteção de dados pessoais insere-se na gama de direitos da personalidade, sendo imprescindível para a LGPD que todos os controladores de dados sejam vigiados, na medida em que vigiam seus usuários, ou seja, é preciso que tenhamos clareza sobre a forma como sedemos nossas informações pessoais, sobre como essas informações são utilizadas e ainda carecemos de uma compreensão sobre como isso nos afeta. Para além da tutela da privacidade, a sociedade de vigilância precisa de uma contrapartida jurídica que proteja o indivíduo na totalidade de sua personalidade, hoje amplamente digitalizada.

4. A CENTRALIDADE DO CONSENTIMENTO PARA A PROTEÇÃO DE DADOS PESSOAIS

[9] A PEC 17/2019 propõe a inserção da proteção de dados pessoais como direito fundamental em nossa Constituição. Mais especificamente, prevê a alteração do inciso XII do art. 5º para a garantia, "nos termos da lei, do direito à proteção dos dados pessoais, inclusive nos meios digitais". Além disso, o projeto insere o inciso XXX ao art. 22, estabelecendo que a competência para legislar sobre proteção e tratamento de dados pessoais passa a ser privativa da União. Até o presente momento a PEC teve seu texto aprovado pelo Senado e segue em tramitação, necessitando da aprovação de 308 deputados.

Eduardo Magrani (2019, p. 19-20), ao tratar sobre os dados na era da hiperconectividade[10], traz à tona a interação entre as pessoas e as máquinas, assim como o processo de conexão e troca entre as próprias máquinas, com algoritmos cada vez mais inteligentes, velozes e com grande capacidade de armazenamento e processamento de dados. Nesse cenário, nossas relações são profundamente modificadas e sofrem cada vez mais interferências tecnológicas, dispostas na Internet das Coisas (*Internet of things*, ou *IoT*), definida como o "conjunto de novos serviços e dispositivos" que interagem entre eles em processos de tratamento de dados, permeados pelo *Big Data,* Inteligência Artificial, conectividade e capacidade computacional.

As redes sociais estão inclusas nesse contexto de infinitas possibilidades tecnológicas. Nossa comunicação amplamente digitalizada, assim como nossas sociabilidades, estruturam uma dinâmica de coleta de dados estritamente ligados à personalidade nas plataformas digitais, os quais fornecemos por meio de simples *"likes"* (curtidas), postagens e compartilhamentos de conteúdos em rede. Nesse sentido, o professor da Universidade da Califórnia, Martin Hilbert, estudioso sobre temas relacionados ao *Big Data*, em entrevista para a BBC Mundo da Espanha, chama a atenção para sua constatação de que com 150 curtidas, os algoritmos de sites como o *Facebook* podem saber mais sobre uma pessoa que seu companheiro, e com 250 curtidas conseguiriam saber mais sobre a pessoa que ela própria.

A sociedade hiperconectada revela a importância de novas regulações, de acordo com as constantes modificações sociais, que reconfiguram a realidade de deveres e direitos, devendo ocorrer uma reavaliação da extensão do dever de segurança nas relações de consumo. Nesse sentido, as redes sociais, enquanto plataformas controladoras de dados devem se enquadrar em sistemas mais intensivos de segurança dos seus usuários, que consomem seus serviços, mesmo que estes estejam mais efetivamente em uma categoria de produto, ao cederem seus dados pessoais, em grande parte responsáveis pela manutenção e lucratividade dessas redes.

Dessa forma, para além de uma cláusula geral de responsabilidade por danos causados aos direitos de outrem, como dispõe o art. 927, parágrafo único do Código Civil[11],

[10] Termo utilizado inicialmente para designar o estado de disponibilidade permanente dos indivíduos em se manterem conectados a internet, mas possui outros desdobramentos, em geral relacionados à conectividade e às interações entre pessoas e máquinas.

[11] Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.

precisamos compreender que as relações estabelecidas no uso das novas tecnologias implicam contextos mais problemáticos, visto que a vigilância sobre nossos dados pessoais pode interferir na busca por empregos, em relações amorosas, em relações financeiras, acordos bancários, na negociação de seguros, na obtenção de planos de saúde *etc*.

Então, o repasse de nossos rastros digitais, ou a falta de segurança no controle de nossos dados, ultrapassa uma simples irresponsabilidade do provedor de serviços, atingindo diversas esferas sociais e pessoais de nossas vidas. Assim sendo, é de extrema importância o recolhimento de um consentimento acerca da captura de nossos dados, sobre a forma como ocorre esse controle e para que e como nossas informações pessoais são utilizadas. Pois, sem isso, não estaríamos protegendo de fato nossa personalidade no ambiente digital. Acompanhando esse entendimento, Barocas e Nissenbaum (2014, p. 49) esclarecem que diante das mais diversas ingerências sobre os dados pessoais, o fluxo informacional torna-se totalmente volátil. Consequentemente, o titular dos dados pessoais deveria ter uma consciência ampla acerca dos processos de tratamentos de dados, para que pudesse gerenciar as suas informações pessoais.

Bruno Bioni (2018, p. 146) destaca um obstáculo crucial para o consentimento nas plataformas digitais, que é a racionalidade limitada do ser humano. O autor enfrenta a questão explicando que não temos certeza sobre a capacidade das pessoas de compreenderem por completo o tratamento de seus dados pessoais:

> Já se faz impossível memorizar os inúmeros atores que compõem a referenciada rede social de publicidade, quanto mais compreender como os dados pessoais serão por eles tratados, já que cada um deles tem as suas respectivas políticas de privacidade. Soma-se, ainda, o complicador da compreensão de como a agregação dos dados pessoais desenrolar-se-á a ponto de extrair informações mais detalhadas sobre seus titulares (BIONI, 2018, p.147).

A LGPD considera o consentimento em seu art. 5º, XII, como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". No entanto, a lei não se concretiza facilmente nos termos de uso e consentimento das redes sociais. Bioni (2018, p. 170) esclarece que há um desenvolvimento incompleto do consentimento, pois este não se estrutura adequadamente

Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

para uma "esfera de controle dos dados pessoais". Assim, o mercado de dados se autorregulou, com o surgimento das políticas de privacidade, que encontramos facilmente nas páginas das mais diversas redes e plataformas digitais. Contudo, o autor indica que essa resposta regulatória tem se mostrado ineficiente, pois apesar de vender-se como uma forma de recolhimento expresso do consentimento, acaba por reforçar a "assimetria do mercado informacional" e configura-se como um mecanismo que não "capacita efetivamente o cidadão para exercer controle sobre as suas informações pessoais".

No que tange à capacidade de controle informacional dos titulares, Ana Frazão (2019b, p. 124) alerta que, apesar da LGPD exigir um consentimento qualificado, as múltiplas negociações com dados impossibilitam a contemplação desse requisito legal. Pasquale (2015) dimensiona essa questão como um pressuposto ficcional, visto que seria improvável que as pessoas passassem a barganhar a privacidade, ou até mesmo que elas se negassem a consumir os serviços para protegerem seus direitos. Desse modo, em um contexto no qual a aceitação dos termos de uso em redes sociais é a condição primordial para sua utilização, as pessoas tendem a acatarem as chamadas cláusulas *take it or leave it* (em tradução livre, "pegar ou largar), que designam essa condição enrijecida, à qual os usuários são submetidos ao acessarem as redes. Assim, ou aceitam todas as disposições contratuais de uso, criadas unilateralmente pelas empresas e apresentadas em uma estrutura de consentimento não dialogal, ou então não podem ser um membro daquele espaço de sociabilidade digital.

O tratamento de dados por meio do consentimento do titular não é a única hipótese legal para o tratamento de dados e nem é hierarquicamente superior às outras formas. No entanto, os princípios que embasam a LGPD demonstram uma centralidade na proteção do ser humano e de sua personalidade. Nesse sentido, o consentimento torna-se central em grande parte dos processos de tratamentos de dados pessoais, o que revela uma preocupação do legislador com a participação do indivíduo no fluxo de suas informações pessoais. A LGPD estabelece em seu art. 7º como o tratamento de dados deverá ocorrer. A lei também diferencia dados pessoais de dados sensíveis, tendo estes um tratamento mais complexo, com maiores exigências legais.

O art. 5º, I determina o dado pessoal como composto por informações relacionadas a pessoa natural identificada ou identificável, já o dado pessoal sensível, disposto no art. 5º, II, se refere à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida

sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Nesse sentido, as redes sociais que abordamos neste trabalho tratam em grande parte, os dados pessoais sensíveis.

No entendimento de Caitlin Mulholland (2018, p. 163), a privacidade evoluiu para incluir em seu conteúdo situações de tutela de dados sensíveis, de seu controle pelo titular e, especialmente, de "respeito à liberdade das escolhas pessoais de caráter existencial". Portanto, a preocupação legislativa com os dados sensíveis, que se referem aos aspectos mais íntimos da esfera privada dos indivíduos, deve abarcar uma compreensão ampla do conceito de privacidade, levando-se em conta as particularidades da proteção de dados pessoais como um direito da personalidade à parte no cenário contemporâneo, no qual o conceito de privacidade ultrapassou a ideia do direito de não ser perturbado, devido ao intenso fluxo de coleta e divulgação de dados na sociedade.

Não obstante, o princípio da não discriminação, contido na LGPD em seu art. 6º, IX é essencial para nortear o tratamento de dados sensíveis, devido ao fato de que o uso desses é potencialmente lesivo, em decorrência de sua capacidade discriminatória, seja por entes privados - *i.e.*, fornecedoras de produtos e serviços - seja por entes públicos. A formação de perfis baseados em dados pessoais sensíveis pode gerar discriminação por diversos fatores, dentre eles o fato de que dados pessoais aparentemente "não sensíveis" podem se tornar sensíveis se contribuem para a elaboração de um perfil, ou ainda em contextos em que a própria esfera individual pode ser violada quando a pessoa pertence a um grupo do qual tenha sido traçado um perfil estigmatizado, ou associado a características e interpretações negativas.

A lei estabelece restrições importantes em casos de tratamento de dados sensíveis. No que tange ao consentimento, a LGPD determina em seu art. 11, inciso I, a necessidade de que o consentimento seja concretizado de forma específica e destacada e para finalidades singulares. Dessa forma, há o reconhecimento de que o consentimento do titular de dados sensíveis deve ser qualificado, por tratar-se de um contratante vulnerável, caracterizado justamente pela ausência de liberdade substancial no momento da determinação da vontade e em um contexto no qual suas informações mais íntimas e invioláveis estão em jogo.

Vale ressaltar que a LGPD permite, em seu art. 11, II, b, o tratamento de dados sensíveis sem o consentimento do titular de dados, quando for indispensável para o tratamento compartilhado de dados pela administração pública para a execução de políticas públicas previstas em leis ou regulamentos, além de outras hipóteses que se referem, em grande parte,

a interesses públicos. Neste último caso, a partir de uma ponderação de interesses, o consentimento do titular dos dados sensíveis seria dispensado pela lei, considerando-se mais relevantes e preponderantes os interesses de natureza pública em detrimento dos interesses do titular, ainda que estes tenham qualidade de direito fundamental. Assim, a lei torna-se passível de críticas, visto que a proteção do conteúdo dos dados pessoais sensíveis é essencial para o pleno exercício dos direitos fundamentais, tais como os da igualdade, liberdade e privacidade.

Gustavo Tepedino e Chiara Spadaccini de Teffe (2019, p. 319-320), discorrem sobre o consentimento na LGPD com ênfase na relevância da lei no atual cenário das novas tecnologias. Os autores expressam que, ao dar enfoque à pessoa e ao livre desenvolvimento de sua personalidade, a lei "assegura o exercício da liberdade existencial e da igualdade material", devido à centralidade da informação nas escolhas individuais e no estabelecimento de vínculos sociais. Desse modo, a expressividade dada ao consentimento pelo legislador incentiva uma participação mais ativa do titular dos dados pessoais nos processos de controle e uso de suas informações, ao passo em que também implica uma maior responsabilidade dos controladores de dados.

5. CONSIDERAÇÕES FINAIS

No início do artigo, propusemos um diálogo com o documentário *Terms and Conditions my apply*, pois sua ideia central, assim como a deste trabalho, é uma compreensão acerca do universo ao qual nos submetemos ao clicarmos em "aceito" ou "estou de acordo" para as cláusulas contratuais inseridas nas políticas de uso e privacidade das redes sociais. A digitalização de nossas relações nos sujeita a vigilância, em sentidos até mais amplos que os indicados por Foucault no passado, pois a caracterização da sociedade de vigilância vive uma constante ampliação dos sentidos de controle e poder sobre os indivíduos através do conhecimento acerca de suas informações pessoais.

Como David Sumpter (2019, p. 41) nos alerta, "estamos clicando nossa personalidade" para dentro de redes como o Facebook, a todo momento, por meio das curtidas, reações, postagens e compartilhamentos. Estamos contando às redes sociais como nos sentimos, do que gostamos e do que não gostamos e revelando nossos desejos de consumo. Tudo isso em um nível que normalmente só partilharíamos com pessoas de extrema confiança como familiares e/ou amigos. As redes sociais estão armazenando, processando e

analisando nosso estado emocional, e é isso o que as alimenta, o que nos torna produtos daquilo que acreditamos sermos clientes.

Dessa forma, os dados pessoais representam importantes contextos existenciais e, portanto, têm sua proteção inserida na gama de direitos da personalidade, sendo classificável como direito fundamental autônomo. Essas características normativas enfatizam a relevância de uma proteção ampla da privacidade, pois para além de uma ideia tradicional de não ser incomodado em sua esfera privativa, o cidadão hoje carece de poder sobre o controle de suas informações pessoais. Ele precisa estar ciente sobre como seus dados podem ser utilizados por entes públicos e privados e participar de forma mais ativa desse processo.

Assim, o consentimento desempenha protagonismo no caráter de proteção da personalidade na Lei Geral de Proteção de Dados Pessoais e nas relações entre controladores de dados e usuários de redes sociais. Nesse contexto, observamos que o consentimento tem o desafio de pautar a autodeterminação informacional das pessoas, conferindo-lhes a oportunidade de participação ativa no tratamento de seus dados. Para tanto, esse consentimento deve ser apresentado da forma mais compreensível possível pelos usuários, que devem ser consultados e alertados sobre a forma como seus dados podem ser, ou estão sendo utilizados. Esse processo deve levar em conta um parâmetro mais protetivo para os dados sensíveis, como estipula a lei, tendo em vista que esta determina que o consentimento para o tratamento de dados sensíveis precisa ser específico e destacado, com finalidades determinadas, uma vez que se tratam de dados relacionados a esferas pessoais extremamente íntimas, que se violadas podem causar graves danos à personalidade e à dignidade humana.

Portanto, o desafio para a adequação do consentimento apresentado nas redes sociais com a LGP está na eficiência dos termos de uso dessas redes para contemplarem um recolhimento do consentimento que capacite os usuários a exercerem a autodeterminação informativa. Desse modo, é preciso que os indivíduos compreendam quais dados estão sendo utilizados pelas redes das quais são usuários, como estão sendo utilizados, por quanto tempo e de quais formas as empresas estão se responsabilizando para garantirem uma esfera digital segura para o livre exercício da personalidade das pessoas, visto que nos encontramos em uma sociedade altamente moldada a partir da vigilância sobre nossos dados pessoais.

REFERÊNCIAS

ARENDT, Hannah. **A condição humana**. Trad. Roberto Raposo. Rio de Janeiro: Forense Universitária, 2010.

BAROCAS, Solon; SELBST, Andrew D. **Big Data's Disparate Impact**. California Law Review, v. 104, p. 2-6. 2016. Disponível em: < http://ssrn.com/abstract=2477899>. Acesso em : 15 jul. 2019.

BAROCAS, Solon; NISSENBAUM, Helen. **Big Data's Run Around Consent and Anonymity**. In: Lane, J.; STODDEN, V.; BENDER, S.; NISSENBAUM, H. (Ed.). Privacy, Big Data and the Public Good. Cambridge: Cambridge University Press, 2014. P. 44-75.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL, Assembleia Legislativa. Lei 13.709/2018. Regulamenta a proteção de dados. Disponível em:«http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm> Acesso em: 23 jul. 2019 .

BRASIL, Assembleia Legislativa. Lei 10.406/2002. Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em 25 jul. 2019.

BRASIL, Assembleia Legislativa. Constituição da República Federativa do Brasil de 1988. Disponível em : <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 24 jul. 2019.

BRASIL, Senado Federal. Proposta de Emenda à Constituição n° 17, de 2019. Disponível em: < https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em 20 ago. 2019.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FRAZÃO, Ana. **Fundamentos da proteção de dados pessoais**. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA , Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1 .ed. São Paulo: Thomson Reuters Brasil, 2019. p. 23-52.

FRAZÃO, Ana. **Objetivos e Alcance da Lei Geral de Proteção de Dados**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA , Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1 .ed. São Paulo: Thomson Reuters Brasil, 2019b. p. 99-129.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 14. ed. Petrópolis: Vozes, 1996.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2007.

HILBERT, Martin. Despreparada para a era digital, a democracia está sendo destruída', afirma guru do big data. Disponível em : < https://www.bbc.com/portuguese/geral-39535650>. Acesso em 15 ago. 2019.

LEVY, Pierre. **A conexão planetária**. O mercado, o ciberespaço, a consciência. Tradução de Maria Lúcia Homem e Ronaldo Entler. São Paulo: Editora 34, 2001.

MAGRANI, Eduardo**. Entre dados e robôs**. Ética e Privacidade na Era da Hiperconectividade. 2.ed. Porto Alegre: Arquipélago Editorial, 2019.

MULHOLLAND, C. **Dados pessoais sensíveis e a tutela de Direitos Fundamentais**. Uma análise à luz da Lei geral de Proteção de Dados (Lei 13.709/18). R. Dir. Gar. Fund., Vitória, 2018, v. 19, n. 3, p. 159-180.

PASQUALE, Frank. **The black box society**. The secret algorithms that control Money and information. Cambridge: Harvard University Press, 2015.

PASQUALINI, Alexandre. **Hermenêutica e sistema jurídico**. Porto Alegre: Livraria do Advogado, 1999.

POULLET, Yves. **About the E-Privacy Directive**. Towards a Third Generation of Data Protection Legislation? In: GUTWIRTH, Serge; POULLET, Yves; HERT, Paul de (Org.). Data Protection in a Profiled World. New York: Springer, 2010.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Il diritto di avere**. Roma: Laterza, 2012.

SOLOVE, Daniel. **Introduction: Privacy self-management and the conset dilema**. Harvard Law Review, v. 126, p. 1880-1903, 2013. Disponível em: <http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf >. Acesso em 15 jun. 2019.

SRNICEK, Nick. **Plataform capitalism**. Cambridge: Polity Press, 2018.

TEPEDINO, Gustavo. **Temas em Direito Civil**. 3. Ed. Rio de Janeiro: Renovar, 2004.

TEPEDINO, Gustavo. **O papel da doutrina no direito civil entre o sujeito e a pessoa**. In: TEPEDINO, Gustavo; TEIXEIRA, Ana Carolina Brochado; ALMEIDA, Vitor (coord.). O direito civil entre o sujeito e a pessoa: estudos em homenagem ao professor Stefano Rodotà. Belo Horizonte: Fórum, 2016. P. 17-35.

TEPEDINO, Gustavo, TEFFÉ, Chiara S. de. **Consentimento e Proteção de Dados Pessoais na LGPD**. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA , Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1 .ed. São Paulo: Thomson Reuters Brasil, 2019. p. 287-322.

TERMS and Conditions my apply. Direção: Cullen Hoback. Produção: Cullen Hoback, John Ramos, Nitin Khanna. Estados Unidos: Variance Films, Hyrax Films, 2013. 80 minutos.

ZUBOFF, Shoshana**. The age of survillance capitalism**. The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.